PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : G06F 12/14

A1

(11) Internationale Veröffentlichungsnummer: WO 00/19321

(43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)

(21) Internationales Aktenzeichen: PCT/EP99/07457

(22) Internationales Anmeldedatum: 27. September 1999 (27.09.99)

(30) Prioritätsdaten:
198 45 097.4 30. September 1998 (30.09.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(71) Anmelder *(nur für DE)*: PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH [DE/DE]; Habsburgerallee 11, D–52066 Aachen (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MÜLLER, Detlef [DE/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Anwalt: PETERS, Carl, H.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR DISABLING DATA AND DATA PROCESSING CIRCUIT FOR CARRYING OUT SAID METHOD

(54) Bezeichnung: VERFAHREN ZUM UNBRAUCHBARMACHEN VON DATEN UND DATENVERARBEITUNGSSCHALTUNG ZUR DURCHFÜHRUNG DES VERFAHRENS

(57) Abstract

The invention relates to a method for disabling data signals, which are stored in a storage arrangement comprised by a data processing circuit, according to selected address signals. These data signals are disabled by a reset signal which is triggered by a singular event in the data processing circuit, in which data and address signals are transmitted to the storage arrangement using at least one code, according to a selected coding process. These codes are changed by the reset signal. The invention also relates to a data processing circuit for carrying out the above–mentioned method. The invention provides a means of reliably disabling the stored data signals when a singular event occurs, using a simple circuit design.

(57) Zusammenfassung

Die Erfindung beschreibt ein Verfahren zum Unbrauchbarmachen von in einer von einer Datenverarbeitungsschaltung umfaßten Speicheranordnung gemäß vorgebbarer Adreßsignale gespeicherten Datensignalen durch ein Rücksetzsignal, welches in der Datenverarbeitungsschaltung von einem singulären Ereignis ausgelöst wird, worin Daten– und Adreßsignale mit Hilfe wenigstens eines Schlüssels nach einem vorgebbaren Verschlüsselungsverfahren der Speicheranordnung zugeführt werden, welche Schlüssel durch das Rücksetzsignal verändert werden. Die Erfindung beschreibt ferner eine Datenverarbeitungsschaltung zum Durchführen dieses Verfahrens. Durch die Erfindung werden die gespeicherten Datensignale zuverlässig mit geringem Schaltungsaufwand beim Auftreten eines singulären Ereignisses unbrauchbar gemacht.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien
AM	Armenien
AT	Österreich
AU	Australien
AZ	Aserbaidschan
BA	Bosnien-Herzegowina
BB	Barbados
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BJ	Benin
BR	Brasilien
BY	Belarus
CA	Kanada
CF	Zentralafrikanische Republik
CG	Kongo
CH	Schweiz
CI	Côte d'Ivoire
CM	Kamerun
CN	China
CU	Kuba
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
EE	Estland
ES	Spanien
FI	Finnland
FR	Frankreich
GA	Gabun
GB	Vereinigtes Königreich
GE	Georgien
GH	Ghana
GN	Guinea
GR	Griechenland
HU	Ungarn
IE	Irland
IL	Israel
IS	Island
IT	Italien
JP	Japan
KE	Kenia
KG	Kirgisistan
KP	Demokratische Volksrepublik Korea
KR	Republik Korea
KZ	Kasachstan
LC	St. Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxemburg
LV	Lettland
MC	Monaco
MD	Republik Moldau
MG	Madagaskar
MK	Die ehemalige jugoslawische Republik Mazedonien
ML	Mali
MN	Mongolei
MR	Mauretanien
MW	Malawi
MX	Mexiko
NE	Niger
NL	Niederlande
NO	Norwegen
NZ	Neuseeland
PL	Polen
PT	Portugal
RO	Rumänien
RU	Russische Föderation
SD	Sudan
SE	Schweden
SG	Singapur
SI	Slowenien
SK	Slowakei
SN	Senegal
SZ	Swasiland
TD	Tschad
TG	Togo
TJ	Tadschikistan
TM	Turkmenistan
TR	Türkei
TT	Trinidad und Tobago
UA	Ukraine
UG	Uganda
US	Vereinigte Staaten von Amerika
UZ	Usbekistan
VN	Vietnam
YU	Jugoslawien
ZW	Zimbabwe

Verfahren zum Unbrauchbarmachen von Daten und Datenverarbeitungsschaltung zur Durchführung des Verfahrens.

Die Erfindung betrifft ein Verfahren zum Unbrauchbarmachen von Daten sowie eine Datenverarbeitungsschaltung zum Durchführen dieses Verfahrens.

Datenverarbeitungsschaltungen, insbesondere in der Form von Microcontrollern, enthalten vielfach eine Speicheranordnung, die als flüchtiger Datenspeicher (RAM) ausgebildet ist. Wird eine derartige Datenverarbeitungsschaltung in sicherheitsrelevanten Anwendungen eingesetzt, beispielsweise für Chipkarten (Smart Cards), kann es erforderlich sein, beim Auftreten bestimmter Ereignisse den Inhalt dieser Speicheranordnung umgehend zu löschen bzw. unbrauchbar zu machen, um einen unberechtigten Zugriff auf diesen Inhalt, d.h. die in der Speicheranordnung gespeicherten Datensignale, wirksam zu verhindern. Dabei sind folgende Fälle denkbar.

Im Falle eines Angriffs auf die Datenverarbeitungsschaltung, d.h. den Microcontroller, sollen die gespeicherten Datensignale aus der Speicheranordnung umgehend gelöscht werden bzw. unbrauchbar sein. In diesem Fall stellt sich der unberechtigte Zugriff auf die Datenverarbeitungsschaltung, d.h. der Angriff, als singuläres Ereignis dar, welches innerhalb der Datenverarbeitungsschaltung ein Rücksetzsignal auslöst. Die Einzelheiten der Erkennung eines Angriffs sind jedoch nicht Gegenstand der vorliegenden Erfindung.

Die in der Speicheranordnung (insbesondere: RAM) gespeicherten Datensignale können auch nach einem Außerbetriebsetzen der Datenverarbeitungsschaltung durchaus in dieser Speicheranordnung gespeichert bleiben. Der Inhalt der Speicheranordnung wird durch das Abschalten der Versorgungsspannung an der Datenverarbeitungsschaltung somit nicht gelöscht. Bei einer Wiederinbetriebnahme der Datenverarbeitungsschaltung sollen die bis dahin gespeicherten Datensignale in der Speicheranordnung jedoch gelöscht werden. Dabei wird von der Voraussetzung ausgegangen, daß auch die Wiederinbetriebnahme als singuläres Ereignis auftritt, durch welches das genannte Rücksetzsignal ausgelöst wird.

Ein einfaches Löschen der Datensignale in der Speicheranordnung ist dann möglich, wenn die Speicheranordnung als löschbares Random Access Memory ausgebildet ist. Dann können zwar alle Datensignale unmittelbar in der Speicheranordnung gelöscht und damit sicher unbrauchbar gemacht werden. Es zeigt sich jedoch, daß der Aufbau eines solchen

löschbaren RAM sehr viel aufwendiger ist als der einer Speicheranordnung, in der die gespeicherten Datensignale auch nach Abschalten der Versorgungsspannung noch erhalten bleiben. Insbesondere, wenn die Speicheranordnung in der Datenverarbeitungsschaltung "eingebettet" sein soll und mit möglichst geringem Schaltungsaufwand herstellbar sein soll, wie dies vorzugsweise für den genannten Anwendungsfall dringend erforderlich ist, zeigt es sich, daß ein einfaches Unbrauchbarmachen der gespeicherten Datensignale nicht möglich ist.

Die Erfindung hat die Aufgabe, ein einfaches Verfahren und eine einfache Datenverarbeitungsschaltung zum Unbraubarmachen von in einer Speicheranordnung der eingangs genannten Art gespeicherten Datensignalen zu schaffen.

Erfindungsgemäß wird diese Aufgabe gelöst durch ein Verfahren zum Unbrauchbarmachen von in einer von einer Datenverarbeitungsschaltung umfaßten Speicheranordnung gemäß vorgebbarer Adreßsignale gespeicherten Datensignalen durch ein Rücksetzsignal, welches in der Datenverarbeitungsschaltung von einem singulären Ereignis ausgelöst wird, worin Daten- und/ Adreßsignale mit Hilfe wenigstens eines Schlüssels nach einem vorgebbaren Verschlüsselungsverfahren der Speicheranordnung zugeführt werden, welche Schlüssel durch das Rücksetzsignal verändert werden.

Dieses Verfahren wird ferner erfindungsgemäß durchgeführt in einer Datenverarbeitungsschaltung mit einer Datenverschlüsselungsschaltung zum Zuführen von Datensignalen und eines (ersten) Schlüssels zum Abgeben verschlüsselter Datensignale, mit einer Adreßverschlüsselungsschaltung zum Zuführen von Adreßsignalen und eines (zweiten) Schlüssels und zum Abgeben verschlüsselter Adreßsignale, und mit einer Speicheranordnung zum Speichern der verschlüsselten Datensignale gemäß der verschlüsselten Adreßsignale.

Bei dem erfindungsgemäßen Verfahren und der erfindungsgemäßen Datenverarbeitungsschaltung werden somit nicht die gespeicherten Datensignale als solche, sondern vielmehr die Zuordnungen zwischen Daten- und Adreßsignalen gelöscht. Dadurch können die gespeicherten Datensignale als solche in der Speicheranordnung erhalten bleiben, sind aber nach Eintritt des singulären Ereignisses nicht mehr brauchbar. Die ordnungsgemäße Verwertung der Datensignale wird erfindungsgemäß dadurch sichergestellt, daß für die Datensignale, die Adreßsignale ober beide ein vorgebbares Verschlüsselungsverfahren beim Speichern der Datensignale in der Speicheranordnung angewandt wird. Zur Durchführung dieses Verschlüsselungsverfahrens wird ein Schlüssel, d.h. ein als Schlüssel dienendes Signal, bereitgestellt. Durch das Auftreten eines singulären Ereignisses wird dieser Schlüssel umgehend derart verändert, daß er für die Zuordnung zwischen den Daten- und Adreßsignalen nicht mehr verwendet werden kann. Damit fehlt die Information, Daten- und Adreßsignale in

einer für die Funktion der Datenverarbeitungsschaltung notwendigen Weise in Korrelation zu setzen. Die Datensignale in der Speicheranordnung sind dann zwar weiterhin dort vorhanden, jedoch nicht mehr brauchbar.

Bei der Erfindung können die Daten- und die Adreßsignale mit demselben Schlüssel, jedoch auch mit verschiedenen Schlüsseln verschlüsselt werden. Dadurch kann in einfacher Weise unterschiedlichen Sicherheitsanforderungen Rechnung getragen werden.

Vorzugsweise wird bei dem erfindungsgemäßen Verfahren der Schlüssel bzw. werden die Schlüssel durch das Rücksetzsignal gelöscht. Für einen anschließenden Betrieb der Datenverarbeitungsschaltung werden dann neue Schlüssel erzeugt. Die Erzeugung der Schlüssel erfolgt bevorzugt durch eine Anordnung mit einer Zufallsfunktion. Auch dies dient der Sicherheit der unbrauchbar zu machenden Daten. Durch diese Maßnahmen ist einerseits der Schlüssel nicht rekonstruierbar, andererseits wird mit geringem Aufwand beim Auftreten des singulären Ereignisses die Zuordnung von Datensignalen und Adreßsignalen in der Speicheranordnung irreversibel aufgehoben.

In einer erfindungsgemäßen Datenverarbeitungsschaltung enthält die Datenverschlüsselungsschaltung bevorzugt einen ersten Schlüsselspeicher zum Speichern des (ersten) Schlüssels, der für die Verschlüsselung der Datensignale eingesetzt wird. Ferner umfaßt die Datenverschlüsselungsschaltung eine erste Verknüpfungsschaltung, in der nach dem vorgebbaren Verschlüsselungsverfahren mit Hilfe des (ersten) Schlüssels die Datensignale verschlüsselt werden. Einen entsprechenden Aufbau weist auch die Adreßverschlüsselungsschaltung mit einem zweiten Schlüsselspeicher und einer zweiten Verknüpfungsschaltung auf. Durch das Rücksetzsignal werden dann lediglich die Schlüssel in den Schlüsselspeichern gelöscht, die Datensignale in der Speicheranordnung müssen dann durch das Rücksetzsignal nicht verändert werden.

Der im ersten Schlüsselspeicher gespeicherte Schlüssel dient außerdem in einer dritten Verknüpfungsschaltung zum Entschlüsseln von der Speicheranordnung abgegebener, verschlüsselter Datensignale. Durch Verändern, insbesondere Löschen des Schlüssels im ersten Schlüsselspeicher wird dann zugleich auch das Auslesen der Datensignale aus der Speicheranordnung in der Weise unterbunden, daß durch die Aufhebung der korrekten Zuordnung ein Auslesen brauchbarer Datensignale nicht mehr möglich ist.

Im Einsatz einer erfindungsgemäßen Datenverarbeitungsschaltung unter Nutzung des erfindungsgemäßen Verfahrens wird dann wir folgt vorgegangen. Nach jeder Inbetriebnahme der Datenverarbeitungsschaltung, bei welcher in Betriebnahme auch ein Rücksetztsignal erzeugt wird, werden die bis dahin gültigen Schlüssel gelöscht bzw. verändert.

Anschließend wird vor der neuen Benutzung der Datenverarbeitungsschaltung, d.h. vor dem erneuten Speichern von Datensignalen in der Speicheranordnung, den Datensignalen, den Adreßsignalen oder beiden ein neuer Schlüssel bzw. werden neue Schlüssel zugewiesen. Dieser Schlüssel kann entweder aus einem Zufallszahlengenerator innerhalb der Datenverarbeitungsschaltung erzeugt oder auch von außerhalb durch Übertragung einer Zufallszahl bereitgestellt werden. Wichtig ist dabei, daß nach jeder Wiederinbetriebnahme der Datenverarbeitungsschaltung über das Rücksetzsignal ein anderer (bzw. andere) Schlüssel verwendet wird (bzw. werden). Die mit dem (bzw. den) Schlüssel(n) in der Speicheranordnung gespeicherten Daten können von der Datenverarbeitungsschaltung jederzeit verwendet werden.

Tritt nun erneut ein Rücksetzsignal auf, wird der bisherige Schlüssel bzw. werden die bisherigen Schlüssel irreversibel zerstört. Die gespeicherten Datensignale sind danach nicht mehr brauchbar, die Funktionsfähigkeit der Datenverarbeitungsschaltung wird jedoch nicht beeinträchtigt, da jederzeit durch Festlegung neuer Schlüssel eine neue Benutzung eingeleitet werden kann.

Ein Beispiel für eine erfindungsgemäße Ausbildung einer Datenverarbeitungsschaltung ist in der Zeichnung dargestellt und wird im nachfolgenden näher beschrieben.

Die einzige Figur der Zeichnung zeigt blockschematisch eine Datenverarbeitungsschaltung 1, die eine Speicheranordnung 2 enthält, die bevorzugt als sogenanntes "eingebettetes RAM" ausgebildet ist. Ein erster Schlüsselspeicher 3 und eine erste Verknüpfungsschaltung 4 bilden gemeinsam eine Datenverschlüsselungsschaltung. Ein zweiter Schlüsselspeicher 5 und eine zweite Verknüpfungsschaltung 6 bilden eine Adreßverschlüsselungsschaltung. Eine dritte Verknüpfungsschaltung 7 dient zum Entschlüsseln der von der Speicheranordnung 2 abgegebenen, verschlüsselten Datensignale.

Im dargestellten Ausführungsbeispiel ist die Speicheranordnung 2 eingerichtet für die Speicherung einer Anzahl von 2^m Datenworten der Wortbreite n. Entsprechend sind die Mehrfachverbindungen der Baugruppen in der Figur gekennzeichnet.

Die Speicheranordnung 2 weist einen Dateneingang 20 zum Zuführen von Datensignalen in der Form von Datenworten der Wortbreite n auf. Die Zuordnung dieser Datenworte zu bestimmten Speicherplätzen innerhalb der Speicheranordnung 2 erfolgt durch Adreßsignale, die als Adreßworte mit einer Wortbreite m an einem Adreßeingang 21 zugeführt werden. An einem Datenausgang 22 können die Datenworte der Wortbreite n wieder abgegriffen werden.

In der vorliegenden Datenverarbeitungsschaltung werden dem Dateneingang 20 der Speicheranordnung 2 verschlüsselte Datensignale zugeleitet. Diese werden aus (unverschlüsselten) Datensignalen gewonnen, die über einen Dateneingang 41 der ersten Verknüpfungsschaltung 4 zugeleitet werden. Die erste Verknüpfungsschaltung 4, Teil der Datenverschlüsselungsschaltung, erhält einen ersten Schlüssel über ihren Schlüsseleingang 40 zugeleitet. In der ersten Verknüpfungsschaltung 4 werden die unverschlüsselten Datensignale nach Maßgabe des ersten Schlüssels über ein vorgebbares Verschlüsselungsverfahren mit einer linearen oder einer nicht linearen Funktion verschlüsselt. Die verschlüsselten Datensignale werden vom Datenausgang 42 der ersten Verknüpfungsschaltung 4 dem Dateneingang 20 der Speicheranordnung 2 zugeleitet.

In entsprechender Weise werden einem Adreßeingang 61 der zweiten Verknüpfungsschaltung 6 die unverschlüsselten Adreßsignale der Wortbreite m zugeleitet. Über einen Schlüsseleingang 60 wird der zweiten Verknüpfungsschaltung 6 ein zweiter Schlüssel zugeführt, der hier die den Adreßworten angepaßte Wortbreite m aufweist, wo hingegen der erste Schlüssel für die Verschlüsselung der Datensignale im gezeigten Beispiel eine Wortbreite n zeigt. Am Adreßausgang 62 werden verschlüsselte Adreßsignale abgegeben.

Der erste Schlüssel wird dem Schlüsseleingang 40 vom Schlüsselausgang 32 des ersten Schlüsselspeichers 3 zugeführt. Der erste Schlüssel wird dem ersten Schlüsselspeicher 3 über einen Schlüsseleingang 30 zugeführt und durch einen Ladebefehl auf einer Steuerleitung 31 im ersten Schlüsselspeicher 3 gespeichert. Durch ein Rücksetzsignal auf einem Rücksetzeingang 33 kann der Inhalt des ersten Schlüsselspeichers 3, d.h. der erste Schlüssel, aus dem ersten Schlüsselspeicher 3 gelöscht werden.

In entsprechender Weise ist der zweite Schlüsselspeicher 5 ausgestattet. Der zweite Schlüssel wird über einen Schlüsseleingang 50 zugeführt und durch einen Ladebefehl auf einer Steuerleitung 51 in den zweiten Schlüsselspeicher 5 eingespeichert. Er ist dann auf einem Schlüsselausgang 52 verfügbar. Durch ein Rücksetzsignal an einem Rücksetzeingang 53 kann der zweite Schlüssel aus dem zweiten Schlüsselspeicher 5 wieder gelöscht werden.

Zum Auslesen der Datensignale aus der Speicheranordnung 2 dient die dritte Verknüpfungsschaltung 7 in Verbindung mit dem ersten Schlüsselspeicher 3. Dabei werden dieselben Schlüssel verwendet wie für das Speichern von Datensignalen. Ein entsprechend durch ein verschlüsseltes Adreßwort adressiertes Datenwort gelangt vom Datenausgang 22 der Speicheranordnung 2 an einen Dateneingang 70 der dritten Verknüpfungsschaltung 7. Das verschlüsselte Datensignal wird in der dritten Verknüpfungsschaltung 7 mit Hilfe des ersten Schlüssels vom ersten Schlüsselspeicher 3, der von dessen Schlüsselausgang 32 an einen

Schlüsseleingang 71 der dritten Verknüpfungsschaltung 7 geführt wird, nach einem vorgebbaren Entschlüsselungsverfahren so entschlüsselt, daß am Datenausgang 72 ein entschlüsseltes Datensignal zur Verfügung steht, welches bevorzugt identisch ist mit dem unverschlüsselten Datensignal am Dateneingang 41 der ersten Verknüpfungsschaltung 4. Auch die dritte Verknüpfungsschaltung 7 kann gemäß einer linearen oder einer nicht linearen Funktion verschlüsseln. Durch Löschen des ersten Schlüssels im ersten Schlüsselspeicher 3 wird somit zugleich auch die Entschlüsselung der verschlüsselten Datensignale unmöglich gemacht.

Die Verknüpfungsschaltungen 4,5,6,7 können beliebige, einander angepaßte Verschlüsselungsverfahren realisieren. In einer Variation der dargestellten Datenverarbeitungsschaltung kann in die Verschlüsselung der Datensignale auch das verschlüsselte Adreßsignal einbezogen werden. Dieses wird dann vom Adreßausgang 62 abgegriffen und einem zusätzlichen Eingang der ersten Verknüpfungsschaltung 4 - -n der Figur nicht dargestellt – zugeleitet.

Die Schlüsselspeicher 3,5 können durch jede löschbare Art von Speicher gebildet sein. Diese können entweder über normale Schreib-Operation oder durch angepaßte Ladeschaltungen mit den gewünschten Schlüsseln beschrieben werden. Nach Löschen dieser Schlüssel durch ein Rücksetzsignal an den Rücksetzeingängen 33 bzw. 53 weisen die Schlüsselspeicher 3,5 den Inhalt Null auf, d.h. an ihren Schlüsselausgängen 32 bzw. 52 liegen entsprechende Signale an.

Die Erfindung bietet gegenüber einer fest verdrahteten Vertauschung von Datensignalen und Adreßsignalen den erheblichen Vorteil einer dynamischen Verschlüsselung, die bei jedem Betriebszyklus der Datenverarbeitungsschaltung geändert wird. Ein Reproduzieren vorheriger Betriebszyklen ist damit auch beim Speichern der Datensignale über einen Betriebszyklus hinaus in der Speicheranordnung nicht möglich.

Gegenüber einer sogenannten Stream-Cipher-Verschlüsselung jedes gespeicherten bzw. ausgelesenen Datensignals wird zwar gemäß der Erfindung nicht jedes Datenwort individuell verschlüsselt, sondern wird vielmehr derselbe Schlüssel bzw. werden dieselben Schlüssel für alle Datensignale bzw. Adreßsignale eines Betriebszyklus angewendet. Jedoch ist der Aufwand für die Erfindung bedeutend geringer. Dadurch lassen sich auch hohe Anforderungen an eine kurze Zugriffzeit ohne Schwierigkeiten erfüllen. Insbesondere durch die zusätzliche Verschlüsselung der Adreßsignale ist eine Reproduzierbarkeit des Inhaltes der Speicheranordnung nach Auftreten eines Rücksetzsignals in der Praxis ausgeschlossen.

PATENTSPRÜCHE:

1. Verfahren zum Unbrauchbarmachen von in einer von einer Datenverarbeitungsschaltung umfaßten Speicheranordnung gemäß vorgebbarer Adreßsignale gespeicherten Datensignalen durch ein Rücksetzsignal, welches in der Datenverarbeitungsschaltung von einem singulären Ereignis ausgelöst wird, worin Daten- und/ Adreßsignale mit Hilfe wenigstens eines Schlüssels nach einem vorgebbaren Verschlüsselungsverfahren der Speicheranordnung zugeführt werden, welche Schlüssel durch das Rücksetzsignal verändert werden.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß die Schlüssel durch das Rücksetzsignal gelöscht und für einen anschließenden Betrieb der Datenverarbeitungsschaltung neue Schlüssel erzeugt werden.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, daß die Schlüssel durch eine Anordnung mit einer Zufallsfunktion erzeugt werden.

4. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, daß von der Datenverarbeitungsschaltung als singuläres Ereignis ein unberechtigter Zugriff oder eine Wiederinbetriebnahme detektiert werden.

5. Datenverarbeitungsschaltung mit einer Datenverschlüsselungsschaltung zum Zuführen von Datensignalen und eines (ersten) Schlüssels zum Abgeben verschlüsselter Datensignale, mit einer Adreßverschlüsselungsschaltung zum Zuführen von Adreßsignalen und eines (zweiten) Schlüssels und zum Abgeben verschlüsselter Adreßsignale, und mit einer Speicheranordnung zum Speichern der verschlüsselten Datensignale gemäß der verschlüsselten Adreßsignale.

6. Datenverarbeitungsschaltung nach Anspruch 5,
dadurch gekennzeichnet, daß die Datenverschlüsselungsschaltung einen ersten Schlüsselspeicher zum Speichern des (ersten) Schlüssels und eine erste

Verknüpfungsschaltung zum Verschlüsseln der Datensignale mit dem (ersten) Schlüssel umfaßt.

7. Datenverarbeitungsschaltung nach Anspruch 5 oder 6,
dadurch gekennzeichnet, daß die Adreßverschlüsselungsschaltung
einen zweiten Schlüsselspeicher zum Speichern des (zweiten) Schlüssels und eine zweite Verknüpfungsschaltung zum Verschlüsseln der Adreßsignale mit dem (zweiten) Schlüssel umfaßt.

8. Datenverarbeitungsschaltung nach Anspruch 5, 6 oder 7,
gekennzeichnet durch eine dritte Verknüpfungsschaltung zum Entschlüsseln von der Speicheranordnung abgegebener, verschlüsselter Datensignale mit dem (ersten) Schlüssel.

1/1

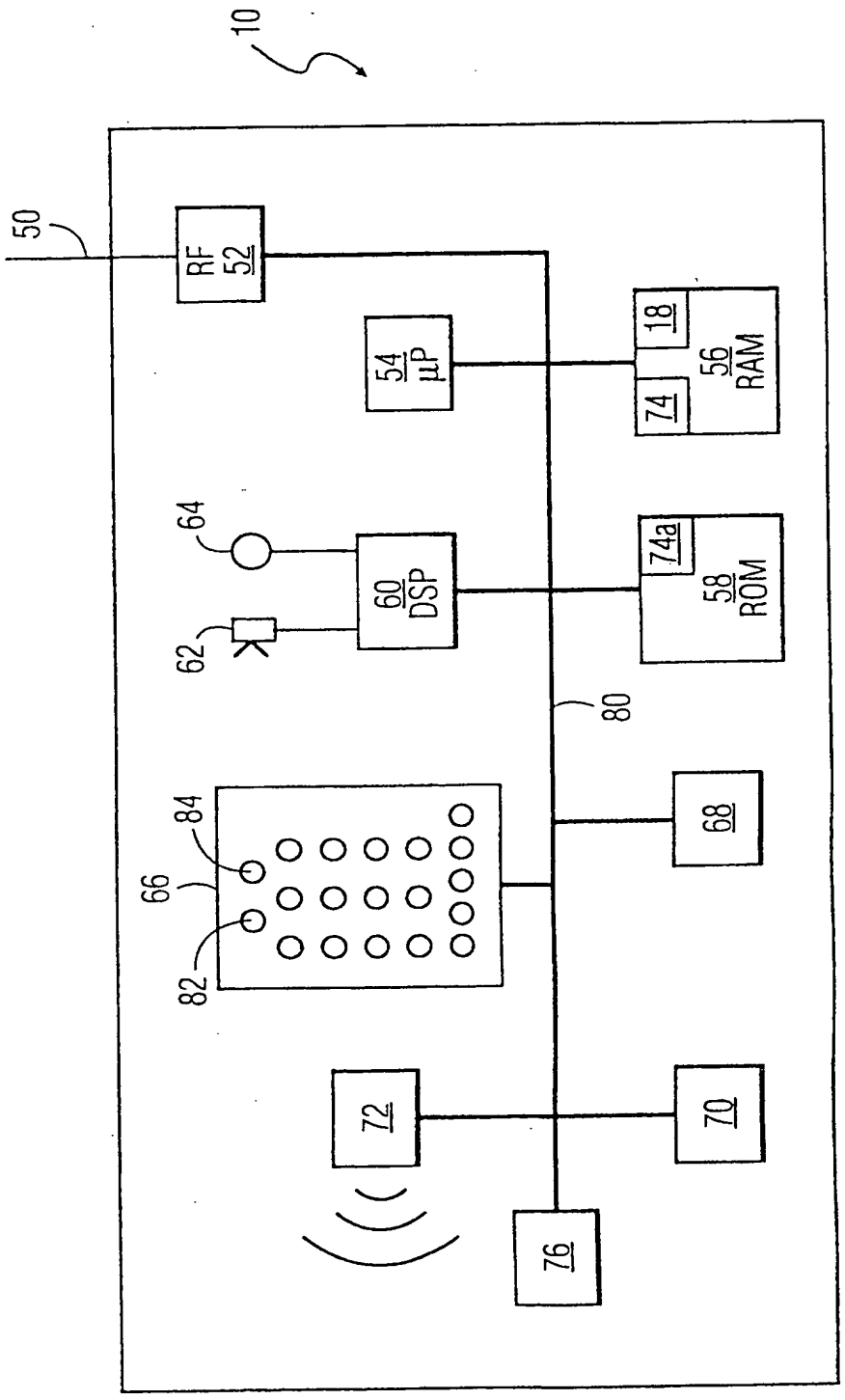

10
50
RF 52
54 µP
18
74
56 RAM
64
62
60 DSP
74a
58 ROM
80
84
66
82
68
72
70
76

FIG. 1

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 99/07457

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 081 675 A (KITTIRUTSUNETORN KITTI) 14 January 1992 (1992-01-14) abstract; figures 2,4,6,7 column 2, line 30 -column 3, line 13 column 5, line 43 -column 6, line 3 claims 1-20	1-8
P,X	WO 98 47060 A (DALLAS SEMICONDUCTOR) 22 October 1998 (1998-10-22) the whole document	1-7
X	DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6 October 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731 the whole document	1-6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 2000	21/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/EP 99/07457

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 457 748 A (BERGUM RUSSELL A ET AL) 10 October 1995 (1995-10-10) abstract; figure 3 column 2, line 33 -column 3, line 19	4

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/EP 99/07457

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5081675 A	14-01-1992	NONE	
WO 9847060 A	22-10-1998	AU 8755698 A	11-11-1998
		ZA 9803108 A	20-10-1998
US 5457748 A	10-10-1995	EP 0671090 A	13-09-1995
		JP 8504067 T	30-04-1996
		WO 9413080 A	09-06-1994

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/07457

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F12/14

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 081 675 A (KITTIRUTSUNETORN KITTI) 14. Januar 1992 (1992-01-14) Zusammenfassung; Abbildungen 2,4,6,7 Spalte 2, Zeile 30 -Spalte 3, Zeile 13 Spalte 5, Zeile 43 -Spalte 6, Zeile 3 Ansprüche 1-20 ---	1-8
P,X	WO 98 47060 A (DALLAS SEMICONDUCTOR) 22. Oktober 1998 (1998-10-22) das ganze Dokument ---	1-7
X	DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6. Oktober 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731 das ganze Dokument --- -/--	1-6

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
11. Februar 2000	21/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/07457

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie²	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 457 748 A (BERGUM RUSSELL A ET AL) 10. Oktober 1995 (1995-10-10) Zusammenfassung; Abbildung 3 Spalte 2, Zeile 33 -Spalte 3, Zeile 19	4

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 99/07457

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5081675 A	14-01-1992	KEINE	
WO 9847060 A	22-10-1998	AU 8755698 A	11-11-1998
		ZA 9803108 A	20-10-1998
US 5457748 A	10-10-1995	EP 0671090 A	13-09-1995
		JP 8504067 T	30-04-1996
		WO 9413080 A	09-06-1994

THIS PAGE BLANK (USPTO)